

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

United States Courts
Southern District of Texas

UNITED STATES DISTRICT COURT

FILED

March 24, 2023

for the
Southern District of Texas

Nathan Ochsner, Clerk of Court

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 IN THE MATTER OF THE SEARCH OF INFORMATION
 ASSOCIATED WITH INSTAGRAM ACCOUNT
 "treyveondadon"

Case No. **4:23-mj-573**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A and the Affidavit in support of search warrant

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B and the Affidavit in support of search warrant

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 Title 18 USC Sec 1591
 Title 18 USC Sec 2422

Sex Trafficking of Minors
 Coercion and Enticement

Offense Description

The application is based on these facts:

See the Affidavit in support of search warrant

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days *(give exact ending date if more than 30 days; _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Brianna Reese*Applicant's signature*

SA Brianna Reese

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
 _____ Telephone *(specify reliable electronic means)*.

Date: 03/24/2023City and state: Bend, OR
Judge's signature

Andrew M. Edison, United States Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

IN RE SEARCH OF:)
INFORMATION ASSOCIATED WITH)
THE INSTAGRAM URL)
<https://www.instagram.com/treyveondadon/>)
THAT IS STORED AT PREMISES)
CONTROLLED BY META PLATFORMS, INC.)
1601 Willow Road, Menlo Park, CA 94025)

4:23-mj-573

Case No.

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

Your Affiant, Brianna Reese, being duly sworn, deposes and says:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for, the Instagram account associated with URL <https://www.instagram.com/treyveondadon/>, UID 56355580720 hereafter referred to as the "TARGET ACCOUNT", which is housed by Meta Platforms, INC. ("Meta"). Meta is a social-networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A), to require Meta to disclose to the government records and other information in its possession, including the contents of communications, pertaining to the subscriber or customer associated with the TARGET ACCOUNT. As set forth herein, there is probable cause to believe that in the TARGET ACCOUNT there exists evidence of a crime in violation of Title 18, U.S.C. §§1591 and 2422, which are further described in Attachment B.
2. I am a Special Agent of the Federal Bureau of Investigation (FBI). I have been a Special Agent of the FBI since October 2022. I am charged with the duty of investigating violations of the laws of the United States, collecting evidence in cases in which the United States is or may

be a party in interest, and performing other duties imposed by law. I am currently assigned to the FBI Houston Human Trafficking Task Force (HTTF) and investigate a variety of human trafficking matters to include Violent Crimes Against Children. Prior to this assignment, I was a Special Agent of the United States Secret Service since 2019. I have been trained in the preparation, presentation, and service of criminal arrest and search warrants and have been involved in the investigation of offenses against the United States to include violent crimes against children and human trafficking offenses.

JURISDICTION

3. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

FACTS AND CIRCUMSTANCES

4. The statements in this affidavit are based upon my investigation, information provided to your Affiant by Special Agents and Task Force Officers (TFO) of the FBI, public source and business records, and my experience and background as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of a crime in violation of Title 18, U.S.C. §1591 (Sex Trafficking) and §2422 (Coercion and Enticement), are currently located in the TARGET ACCOUNT. The evidence of a crime in violation of the aforementioned statutes includes but is not limited to communications related to sex trafficking.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of Title 18, U.S.C. §1591 which states:

(a) Whoever knowingly-

(1) in or affecting interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, recruits, entices, harbors, transports, provides, obtains, advertises, maintains, patronizes, or solicits by any means a person; or

(2) benefits, financially or by receiving anything of value, from participation in a venture which has engaged in an act described in violation of paragraph (1), knowing, or, except where the act constituting the violation of paragraph (1) is advertising, in reckless disregard of the fact, that means of force, threats of force, fraud, coercion described in subsection (e)(2), or any combination of such means will be used to cause the person to engage in a commercial sex act, or that the person has not attained the age of 18 years and will be caused to engage in a commercial sex act.

6. This investigation concerns alleged violations of Title 18, U.S.C. §2422, Coercion and Enticement:

(a) Whoever knowingly-

(1) Persuades, induces, entices, or coerces any individual to travel in interstate or foreign commerce, or in any Territory or Possession of the United States, to engage in prostitution, or in any sexual activity for which any person can be charged with a criminal offense, or attempts to do so. . .

BACKGROUND ON INSTAGRAM

7. From my review of publicly available information provided by Meta about its service, including Meta's "Privacy Policy," I am aware of the following about Meta and about the information collected and retained by Meta.
8. Meta owns and operates a free-access social-networking website named Instagram that can be accessed at <http://www.instagram.com>. Instagram allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and other information. Users can access Instagram through the Instagram website or by using a special electronic application ("app") created by the company that allows users to access the service through a mobile device.
9. Instagram permits users to post photos to their profiles on Instagram and otherwise share photos with others on Instagram, as well as certain other social-media services, including Flickr and Twitter. When posting or sharing a photo on Instagram, a user can add to the photo: a caption; various "tags" that can be used to search for the photo (e.g., a user made add the tag #vw so that people interested in Volkswagen vehicles can search for and find the photo); location information; and other information. A user can also apply a variety of "filters" or other visual effects that modify the look of the posted photos. In addition, Instagram allows users to make comments on posted photos, including photos that the user posts or photos posted by other users of Instagram. Users can also "like" photos.
10. Upon creating an Instagram account, an Instagram user must create a unique Instagram username and an account password. This information is collected and maintained by Meta.
11. Instagram asks users to provide basic identity and contact information upon registration and allows users to provide additional identity information for their user profile. This information may include the user's full name, e-mail addresses, and phone numbers, as well as

potentially other personal information provided directly by the user to Instagram. Once an account is created, users may also adjust various privacy and account settings for the account on Instagram. Meta collects and maintains this information.

12. Instagram allows users to have “friends,” which are other individuals with whom the user can share information without making the information public. Friends on Instagram may come from either contact lists maintained by the user, other third-party social media websites and information, or searches conducted by the user on Instagram profiles. Meta collects and maintains this information.

13. Instagram also allows users to “follow” another user, which means that they receive updates about posts made by the other user. Users may also “unfollow” users, that is, stop following them or block the, which prevents the blocked user from following that user.

14. Instagram allow users to post and share various types of user content, including photos, videos, captions, comments, and other materials. Meta collects and maintains user content that users post to Instagram or share through Instagram.

15. Instagram users may send photos and videos to select individuals or groups via Instagram Direct. Information sent via Instagram Direct does not appear in a user’s feed, search history, or profile.

16. Users on Instagram may also search Instagram for other users or particular types of photos or other content.

17. For each user, Meta also collects and retains information, called “log file” information, every time a user requests access to Instagram, whether through a web page or through an app. Among the log file information that Meta’s servers automatically record is the particular web requests, any Internet Protocol (“IP”) address associated with the request, type of browser used,

any referring/exit web pages and associated URLs, pages viewed, dates and times of access, and other information.

18. Meta also collects and maintains “cookies,” which are small text files containing a string of numbers that are placed on a user’s computer or mobile device and that allows Meta to collect information about how a user uses Instagram. For example, Instagram uses cookies to help users navigate between pages efficiently, to remember preferences, and to ensure advertisements are relevant to a user’s interests.

19. Meta also collects information on the particular devices used to access Instagram. Meta may record “device identifiers,” which includes data files and other information that may identify the particular electronic device that was used to access Instagram.

20. Meta also collects other data associated with user content. For example, Meta collects any “hashtags” associated with user content (i.e., keywords used), “geotags” that mark the location of a photo and which may include latitude and longitude information, comments on photos, and other information. Meta also may communicate with the user, by email or otherwise. Meta collects and maintains copies of communications between Instagram and the user.

DYNAMICS OF DOMESTIC SEX TRAFFICKING

21. Based on my training, and the knowledge, experience, and training of other law enforcement officers, with whom I have consulted, I know that individuals who engage in the sex trafficking of adults and minors, often maintain evidence of their criminal activities in their residences, hotel/motel rooms, other locations that are used as residences and locations associated with their criminal activities. Additional evidence is often found in vehicles, on computers, cellular phones, hard drives, or digital storage devices, and on cameras.

22. Based on my training, I know that individuals that engage in criminal activities, such as sex trafficking, often utilize cellular phones and digital computer devices to maintain constant contact with victims, verify a victim's location through geographic location applications, and instruct them where to meet for sex dates and, more recently use smartphone applications like Venmo, Google Pay, Cash App, Apple Pay and others to accept, transfer, and manage the money exchanged for sex services. These electronic devices are frequently associated with both social activities and their sex trafficking business activities (as they are often intermingled) and often contain evidence of criminal activity; including records of sex dates, contracts with solicitors ("johns"), victims or traffickers ("pimps"), photographs, advertisements, financial records, hotel/motel reservations and receipts, and financial transfers to satisfy their contracts or quotas. The electronic devices also maintain names and contact information of victims and co-conspirators, records and receipts of their crimes, emails, text messages and other records relating to when and where they have participated in illegal activities. Various applications are often downloaded on the cellular phones of the traffickers and their victims to make sex trafficking operations easier such as Whatsapp, Instagram, Snapchat, Uber and Lyft.

23. Based on my training and experience, computers and cellular phones are often essential tools for facilitating human trafficking and online prostitution activity. Social media accounts and text messaging applications are often used to create and maintain the trafficker's persona, recruit victims, document the trafficker's activities, and to boast about their criminal activities. Further, traffickers and their victims use cellular and computer devices to create, review and post online advertisements for sexual services which often contain photographs of victims in sexually explicit poses while wearing provocative clothing.

24. Cellular phones and digital electronic devices belonging to sex traffickers (pimps and johns), their co-conspirators and their victims often contain information ranging from contact names and phone numbers to text messages, emails, login information, GPS location data, photos and notes pertaining to criminal activities associated with the sex trafficking business. Further, perpetrators of sex trafficking crimes frequently have more than one cellular phone to conduct these activities. It is not unusual for traffickers, co-conspirators, and victims to have multiple cellular phones. The traffickers and co-conspirators may also utilize multiple devices and it is common for them to dispose of their cellular phones, or the sim card, and acquire new ones in an attempt to destroy evidence and to avoid or evade encounters with law enforcement.

25. Based on my training and experience, trafficking solicitors, victims, and their pimps typically communicate with each other through cellular phones and/or other electronic devices to include social media to discuss availability, times, prices or quotes for sex acts, quotas, victim location if they are with johns and other matters related to commercial sex acts. With younger or minor victims, it is also common for the traffickers to start “grooming” their victims online for several weeks or even months before the victim engages in a sex act because it can take time to convince the victims to engage in sex acts with strangers.

26. In addition to the use of cellular devices to communicate and document sex trafficking activities, traffickers often use their cellular phones to threaten and control their victims. Traffickers often control victims by tracking their location and scheduling rides to and from sex dates.

27. Individuals that are engaged in sex trafficking often use violence and manipulation to maintain control of their trafficking victims. They often have rules and forms of discipline that are used to maintain order and compliance by the victims. Sometimes these rules are written and

posted for the victims. The posting can be actual posting in a physical location or via cellular device such as in a text or social media message. At other times, the pimps leave their most reliable prostitute, commonly referred to as the “bottom bitch” in charge. Part of the manipulation and coercion often includes the pimps or co-conspirators brandishing weapons, mainly firearms, to scare and intimidate the victims. These weapons are often found in the residences and vehicles frequented by traffickers. They are often also seen in social media posts.

28. In addition, Your Affiant knows that persons engaged in sex trafficking and other criminal activity keep weapons, cellular and digital devices, and other indicia of their criminal activities in residences, vehicles, and hotel/motel rooms that they are associated with both socially and through their illegal business activities. These items include, but are not limited to, list of clients or johns, session sheets, timecards, “trick” books, photographs, advertisements, records of purchases, lists of debts owed, list of work required/quotas, employment applications, financial records, proof of travel, payments and wire transfers.

29. Individuals engaged in sex trafficking often use residences, relatives’ residences, or hotel/motel rooms as a base of operations for their criminal activity. At these locations, victims are often housed and taught, by the trafficker or others engaging in commercial sex, how to engage in commercial sex. These locations are often used as a place for victims to eat, sleep, bathe, and recover from injuries inflicted by the trafficker as well as a place to wait between the times they are engaging in commercial sex acts. These residences are often in suburban areas that would not be associated with commercial sex. To protect their identity and the location of their home the traffickers typically do not allow commercial sex to occur at these locations. However, it is common for the trafficker to engage in sex with the victims at these locations. These locations are also used to store items commonly used by those engaging in commercial

sex such as personal lubricant, condoms, wipes, douche, and other personal hygiene items. Often these items are purchased in bulk and distributed to the victims at the base of operations. Typically, the victims also store their “work clothes” and shoes at these locations.

PROBABLE CAUSE

30. On January 18, 2023, your Affiant learned that Houston Police Department (HPD) recovered a thirteen-year-old Minor Victim (MV1), Date of Birth 08/11/2009, from 9600 Plainfield Street, Houston, Texas 77036. MV1’s identity is known to law enforcement but is not being disclosed because MV1 is a minor. This location is commonly referred to as “The Bissonnet Track” and is a known area for prostitution in Harris County, Texas. Your Affiant obtained a copy of the HPD police report from the December 8, 2022, encounter with MV1. The HPD report disclosed the following information. MV1 was taken to Texas Children’s Hospital for a SANE exam upon recovery. On that same day, MV1 provided the following information to Houston Police Department Vice Division Human Trafficking Unit on call Detective Rosas. MV1 was walking the track because it was “easy money”. MV1’s friend (First Name Unknown, Last Name Unknown) told MV1 about Bissonnet and educated MV1 on what to do while waking “the track”. MV1 was coached both face to face and over the phone. MV1 has been to the track three times and has been on four dates with “johns” and engaged in oral sex with them. MV1 usually charges the “johns” \$150. A “john” is a slang term that is used to refer to a prostitute’s client or solicitor of sex. Law enforcement verified that MV1 has been in runaway status since November 29, 2022.
31. At the time the phone was recovered, MV1 gave HPD the password for the phone, which was provided to your Affiant. MV1 gave both verbal and written consent to Detective Rosas to look through the phone that was in MV1’s care, custody, and control of at the time of

recovery. While examining the phone, Detective Rosas identified a text thread between MV1 and a contact listed as “Daddy (with a king emoji)” with phone number 832-310-0760 from that same day on December 8, 2022. In the text thread, there were two text messages from “Daddy” that stated, “just tell them u a runaway” and “U by yourself and delete our message”. Both text messages were sent at 6:43 PM. MV1 was stopped by HPD patrol officer at approximately 6:39 PM. MV1 stated that “Daddy” was MV1’s fifteen-year-old boyfriend (Jordan Last Name Unknown) and the reason why MV1 deleted the previous text messages with him was because “MV1 sends him nudes” and mentioned that “they fuck”. Through law enforcement database checks, “Daddy” was identified as Trayveon Prater (Date of Birth 11/16/1998). Additionally, phone number 832-310-0760 is the same phone number that Prater gave to HPD in August of 2022 in a burglary report where he is listed as the complainant. Prater was also logged into the iPhone’s iCloud account and the phone was listed as “Treyveon’s iPhone.” However, contact information for the iPhone was listed under MV1’s street name “Cupcake” with phone number 832-709-8929. “Cupcake” is also the name MV1 initially gave to the HPD patrol officer when he first approached MV1.

32. Within the Snapchat application on MV1’s phone, a thread of saved Snapchat messages were observed that were sent between Snapchat user “troy_pomp” (display name “Trigga Trey”) and MV1’s snapchat username “kashbaby.niss” (display name: “lulmama.niss”). Several messages show Prater coaching MV1 on how to be a good prostitute. Messages include the following: “make sure you use the condom and send me the hotel when you get there”, “ima show u how to double yo money so by the time u 18/19 u got yo own crib got your own car”, “don’t forget to handle that stuff for daddy”, “okay good, when I pick u up we going straight to the mall to get u a hoe outfit and a jacket we going hard tn.”, “This is a

old video I found but look at this pimp tryna talk to this hoe u see she keep tryna turn around. She never look at him (100 emoji) that's how u stay loyal to yo pimp".

33. In addition to the Snapchat messages, a video was found in the "recently deleted" album of MV1's iPhone. This video was taken on December 6, 2022. This video shows MV1 naked in a bathtub in which she appears to be disoriented and intoxicated. In this video, you can hear a male talking to MV1. This male's voice is consistent with Prater's voice in a second video recorded the following day on December 7, 2022. In this video, Prater appears to be yelling at his dogs and addresses MV1 by MV1's true name.
34. Within the Instagram application on MV1's phone, MV1 was signed into account "kash.babyy.niss". A screenshot taken of a post from TARGET ACCOUNT was also found on MV1's phone. The post stated, "I be remembering them days I was broke nobody gave me shit. Fuccem we up now". This post was re-posted to MV1's Instagram account with the caption, "(heart eye emoji) daddy".
35. Your affiant conducted open-source research on TARGET ACCOUNT. An extensive number of posts on his story were observed related to prostitution, drugs, and guns. On January 25, 2023, an Instagram story posted to TARGET ACCOUNT of Prater saying, "Yeah you know what's good for you hoe. You wanna fuck with a nigga with some motion. You wanna listen to a pimp with some instruction. Bitch that fee double hoe. I'm just letting you know. Cause I know you finna look at this story. Don't come up in my story. Don't come up in my dms talkin reckless. We take cash, Cash App, Zelle, Apple Pay, all that hoe. Yeah. That way. The fuck. I don't gotta beat my hoes. My hoes listen. They know what the fuck is going on. You listen or your fired. Its that simple. I don't need no bitch." This video was posted to TARGET ACCOUNT's Instagram story with the caption, "I'm not captain save a hoe IAN LETTING SHIT SLIDEE [king emoji] [star emoji]".

36. Prater has posted on TARGET ACCOUNT numerous stories advertising that he is a pimp and is currently taking applications. Prater posted a picture of a female fanning out US currency holding a purse with the caption “trapstars only”. The purse in this picture is the same purse MV1 was wearing when she was recovered by HPD. An additional post shows a female with her face covered and bent over in front of Prater with a song attached titled, “I need a 304”. “304” is a slang term for “a hoe”. This picture is the same picture that MV1 had saved in her Snapchat messages with Prater that he sent to MV1 saying, “always use my king emoji”.

37. On December 15, 2022, the FBI served Meta with a preservation request pursuant to 18 U.S.C. § 2703(f), requiring Instagram to preserve all information associated with the TARGET ACCOUNT, <https://www.instagram.com/treyveondadon/>. The case number provided to the FBI following the request is 7429615. As of February 13, 2023, it appears the TARGET ACCOUNT was deactivated by META.

38. As explained herein, information stored in connection with an Instagram account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, an Instagram user’s account activity, IP log, stored electronic communications, and other data retained by Meta, can indicate who has used or controlled the Instagram account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the Instagram account at a relevant time. Further, Instagram account activity can show how and when the account was

accessed or used. For example, as described herein, Instagram logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Instagram access, use, and events relating to the crime under investigation. Additionally, Meta builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Instagram “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Instagram account owner. Last, Instagram account activity may provide relevant insight into the Instagram account owner’s state of mind as it relates to the offense under investigation. For example, information on the Instagram account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

CONCLUSION

39. Based on the information above, the computers of Meta are likely to contain all the material described above with respect to the TARGET ACCOUNT, including stored electronic communications and information concerning subscribers and their use of Instagram, such as account access information, which would include information such as the IP addresses and devices used to access the account, as well as other account information that might be used to identify and locate the actual user or users of the account at particular times.

40. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular Title 18, U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A), by using the warrant to require

Meta to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

41. Based on the forgoing, I request that the Court issue the proposed search warrant.

42. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta. Because the warrant will be served on Meta, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Brianna Reese

Brianna Reese
Special Agent
Federal Bureau of Investigation

Subscribed and sworn before me, telephonically, this 24th day of March 2023, and I find probable cause.



Honorable Andrew M. Edison
United States Magistrate Judge

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Instagram account associated with the URL: <https://www.instagram.com/treyveondadon/> that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, INC, headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, INC.

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. §2703(f), Meta, is required to disclose the following information to the government for each account listed in Attachment A:

- a. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, phone numbers, gender, hometown, occupation, and other personal identifiers;
- b. All past and current usernames associated with the account;
- c. The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;
- d. All activity logs including IP logs and other documents showing the IP address, date, and time of each login to the account, as well as any other log file information;
- e. All information regarding the particular device or devices used to login to or access the account, including all device identifier information or cookie information, including all information about the particular device or devices used to access the account and the date and time of those accesses;
- f. All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;
- g. All communications or other messages sent or received by the account from November 1, 2022- Present;
- h. All user content created, uploaded, or shared by the account, including any comments made by the account on photographs or other content from November 1, 2022- Present;
- i. All photographs and images in the user gallery for the account from November 1, 2022- Present;
- j. All location data associated with the account, including geotags from November 1, 2022- Present;

- k. All data and information that has been deleted by the user from November 1, 2022- Present;
- l. A list of all of the people that the user follows on Instagram and all people who are following the user (*i.e.*, the user's "following" list and "followers" list), as well as any friends of the user;
- m. A list of all users that the account has "unfollowed" or blocked;
- n. All privacy and account settings;
- o. All records of Instagram searches performed by the account, including all past searches saved by the account from November 1, 2022- Present;
- p. All information about connections between the account and third-party websites and applications; and,
- q. All records pertaining to communications between Meta and any person regarding the user or the user's Instagram account, including contacts with support services, and all records of actions taken, including suspensions of the account.

Meta is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, U.S.C. §1591 and §2422 involving the TARGET ACCOUNT since November 1, 2022, including, for each username identified on Attachment A. Evidence indicating how and when the Instagram account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Instagram account owner;

- (a) Evidence indicating the Instagram account owner's state of mind as it relates to the crime under investigation;
- (b) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

- (c) The identity of the person(s) who communicated with the user ID about matters relating to commercial sex trafficking, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Meta Platforms, Inc., and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Meta Platforms, Inc. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Meta Platforms, Inc., and they were made by Meta, Inc., as a regular practice; and

b. such records were generated by Meta Platforms, Inc.'s, electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Meta Platforms, Inc., in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Meta, Inc., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature